AO 91 (Rev. 11/11) Criminal Complaint (Rev. by USAO on 3/12/20) ☐ Original ☐ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Central District of California

United States of America

v.

Ionut Calciu, Florian Serban,

Defendants

Case No. 2:25-mj-00451-DUTY

CRIMINAL COMPLAINT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date of February 2, 2025 in the County of Los Angeles in the Central District of California, the defendants violated:

Code Section	*Offense Description*
18 U.S.C. § 1029(a)(2)	Use of Unauthorized Access Devices

This criminal complaint is based on these facts:

Please see attached affidavit.

☒ Continued on the attached sheet.

/s/
Complainant's signature

Caitlin Donovan, HSI Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: 2/3/2025

Judge's signature

City and state: Los Angeles, California

Hon. Margo A. Rocconi, U.S. Magistrate Judge
Printed name and title

AUSA: Alexander H. Tran (x0758)

AFFIDAVIT

I, CAITLIN DONOVAN, being duly sworn, declare and state as follows:

I. PURPOSE OF AFFIDAVIT

1. This affidavit is made in support of a criminal complaint against Ionut Calciu ("CALCIU") and Florian Serban ("SERBAN") for a violation of 18 U.S.C. § 1029(a)(2) (use of unauthorized access devices).

2. This affidavit is also made in support of an application for a warrant to search the following digital devices (collectively, the "SUBJECT DEVICES"), in the custody of the United States Secret Service ("USSS"), in Los Angeles, California, as described more fully in Attachment A:

a. A black Apple iPhone, unknown model, unknown serial number, retrieved from CALCIU's person on or about February 2, 2025, ("SUBJECT DEVICE 1");

b. A black Apple iPhone, unknown model, unknown serial number, retrieved from SERBAN's person on or about February 2, 2025 ("SUBJECT DEVICE 2").

3. The requested search warrants seek authorization to seize evidence, fruits, or instrumentalities of violations of 18 U.S.C. §§ 371 (Conspiracy), 1028A (Aggravated Identity Theft), 1029 (Fraud and Related Activity in Connection with Access Devices), and 1344 (Bank Fraud) (collectively, the "Subject Offenses"), as described more fully in Attachment B. Attachments A, and B are incorporated herein by reference.

4. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint and search warrants and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

II. BACKGROUND OF AFFIANT

5. I am a Special Agent ("SA") with Homeland Security Investigations ("HSI") and have been so employed since January 2024. Prior to this position, I was a Customs and Border Protection Officer at the seaport of Long Beach, CA for approximately three years. As a Special Agent, I am responsible for investigating violations of federal criminal laws relating to financial institution fraud, credit card fraud, bank fraud, cybercrimes, and identity theft, among other federal violations. I am a graduate of the Criminal Investigator Training Program conducted at the Federal Law Enforcement Training Center, as well as the Homeland Security Investigations ("HSI") Special Agent Training Course in Glynco, Georgia. I currently work with the El Camino Real Financial Crimes Task Force and have participated in multiple investigations in connection with fraud and cybercrimes.

III. SUMMARY OF PROBABLE CAUSE

6. Between January 2024 and January 1, 2025, the California Department of Social Services ("DSS") has detected more than $126.8 million in stolen funds from victim Electronic Benefit Transfer ("EBT") cards. This fraud is from two specific programs known as CalFresh and CalWORKs, which help low-income households pay for housing, food, and other necessary expenses. Many of the fraudulent withdrawals are done at specific ATMs in the Central District of California.

7. On or about February 2, 2025, at approximately 6:30 a.m. (PST), law enforcement conducted physical surveillance at a U.S. Bank ATM terminal located at 11661 San Vicente Boulevard, Los Angeles, California, which was identified by law enforcement as one of the top 30 ATM U.S. Bank locations for EBT-CalFresh fraud.

8. At approximately, 6:30 a.m., law enforcement saw CALCIU and SERBAN arrive in a white Volvo automobile (the "white Volvo") and proceed to the ATM terminal located at the U.S. Bank branch where law enforcement was conducting surveillance. At the ATM, law enforcement observed, and U.S. Bank confirmed that, CALCIU withdrew cash from the ATM in rapid succession using approximately two different access devices. CALCIU pocketed the withdrawn cash, totaling $1,300. SERBAN was identified by law enforcement as the driver in the white Volvo and was later found in possession of approximately sixty-one different access devices, of which approximately fifty-eight were cloned with

California EBT card numbers. CALCIU and SERBAN were arrested and found possessing the SUBJECT DEVICES.

IV. STATEMENT OF PROBABLE CAUSE

9. Based on my review of law enforcement reports, conversations with other law enforcement agents, and my own knowledge of the investigation, I am aware of the following:

A. Regulatory Background of CalFresh and CalWORKs Programs

10. DSS is a government agency that administers several benefit and assistance programs for residents of the state of California. One of the assistance programs administered by DSS is called CalFresh (formerly known as food stamps), which helps low-income households purchase food and household items to meet their nutritional needs. Another assistance program administered by DSS is called CalWORKs, which helps low-income families with children pay for housing, food, and other necessary expenses.

11. Residents of California that meet the criteria established by the CalFresh or CalWORKs programs can apply online for benefits at www.getcalfresh.org and www.benefitscal.com. Beneficiaries apply for benefits by submitting their income and number of dependents to determine their benefit eligibility.

12. CalFresh and CalWORKs benefits are issued through Electronic Benefit Transfer cards ("EBT cards"). EBT cards are mailed to an address designated by the account holder and function like traditional debit cards to conduct transactions.

For example, you can use an EBT card to make a purchase at a grocery or convenient store by swiping the card at a point-of-sale terminal.

13. The EBT cards issued under CalFresh and CalWORKs are assigned specific Bank Identification Numbers ("BIN"). A BIN refers to the first five digits of the account number on a debit or credit card and can be used to identify the issuer of the card, like DSS, which administers the CalFresh and CalWORKs programs.

14. Benefits received through the program are typically disbursed to EBT cardholders by DSS during the early days of each month. Those benefits are deposited directly from DSS into the account of the EBT cardholder.

15. The EBT cardholders can then conduct cash withdrawals at automated teller machines ("ATMs") using a personal identification number ("PIN") established by the card holder. The EBT cardholder presents the card at an ATM, inserts the card into the ATM card reader, and utilizes a PIN to withdraw the funds previously deposited by DSS intended for beneficiaries of the CalFresh or CalWORKs programs.

B. Background on EBT Fraud in Los Angeles Area and Prior Operation

16. Since in or about August 2022, local law enforcement has been working with DSS to investigate a significant increase in unauthorized cash withdrawals utilizing EBT cards. Based on analysis of victim complaints to DSS, victim complaints to local law enforcement, bank records, and surveillance, law enforcement

determined that the majority of the unauthorized cash withdrawals were being conducted with cloned cards.

17. A cloned card can be a blank white plastic card or another debit, credit or gift card that contains altered information on the card's magnetic stripe. Based on my training and experience, I know that suspects will often clone cards by taking stolen card information from a victim card's magnetic stripe and re-encode that stolen information onto another card's magnetic stripe. Cloning these cards allows the suspect to use the card and the DSS benefits added on to the account linked to the card for illicit purchases or unauthorized cash withdrawals.

18. On a legitimate debit or credit card, the information coded on the card's magnetic stripe will match the information embossed on the front of the card. This information includes the account number, expiration date, and cardholder's name, among other information. Whereas on a cloned card, the information coded on the magnetic stripe will not match the information embossed on the front of the card. For example, if a suspect re-encodes victim EBT card information onto a pre-existing gift card's magnetic stripe or a blank white plastic card with a magnetic stripe, the magnetic stripe will be coded with the EBT card information, but the card itself will still bear the information of the gift card or bear no information if it is a blank white plastic card.

19. Based on my training, experience, and participation in this investigation, I know that the victim card data harvested

to clone cards is often obtained from what is colloquially referred to as "skimming activity."

20. The term "skimming" is used to describe activity that involves unlawfully obtaining debit and credit card information by using technological devices to surreptitiously record victim accountholder's debit and credit card numbers and personal identification numbers at, for example, ATMs or point-of-sale terminals. For example, individuals conducting ATM "skimming" may install a skimming device into the card reader of the ATM to record the debit or credit card numbers, as well as a camera or keypad overlay on the ATM keypad to record the associated PIN number. Those individuals will then return to the ATM to collect the card number and PIN information stored on the installed device.

21. As described above, suspects then manufacture cloned and fraudulent debit or credit cards that bear the victim accountholder's account information that was obtained from skimming. Once that information is loaded onto another fraudulent card (e.g., a gift card or blank plastic card), members of the scheme then use that fraudulent card to withdraw cash from the victim accountholder's bank accounts or to make purchases with the victim accountholder's account.

22. In or about September 2022, local law enforcement conducted a surveillance and arrest operation in the Los Angeles, California area. This operation was planned in response to the large number of unauthorized withdrawals occurring at ATMs in the Los Angeles area during a short period

of time. Specifically, law enforcement had analyzed fraudulent EBT withdrawal data and noticed a high volume of unauthorized withdrawals on specific dates and times that coincided with the dates when the majority of benefits are disbursed to EBT cardholders.

23. As a result of this operation, local law enforcement established surveillance at select Bank of America ATMs that were used to conduct a significant volume of CalFresh fraud. Law enforcement surveilled those ATMs around the dates when benefits had been disbursed, observed suspects that withdrew a high volume of unauthorized withdrawals and that conducted those withdrawals in rapid succession, and arrested multiple individuals believed to be making fraudulent withdrawals of CalFresh benefits. As a result, law enforcement arrested approximately 16 suspects. All of the arrested suspects were later determined to be citizens of countries other than the United States who did not have documentation to be lawfully present in the United States. All of the individuals arrested were released from local custody within hours of their arrest and absconded from any future judicial proceedings.

24. In or about February 2023, in response to a further increase in unauthorized cash withdrawals utilizing EBT cards after the local law enforcement September 2022 operation, federal law enforcement conducted a similar surveillance and arrest operation in the Los Angeles, California area. Law enforcement established surveillance around the dates when benefits had been disbursed at select high-volume EBT fraud

ATMs. Law enforcement arrested three suspects that withdrew a high volume of unauthorized withdrawals and that conducted those withdrawals in rapid succession. Two of those defendants came to the ATM together, possessed 35 cloned EBT cards at the time of arrest, and later analysis of historic ATM surveillance data showed that they had made more than $190,000 in past attempted fraudulent EBT withdrawals from a single bank since October 2022. One additional defendant possessed 269 cloned EBT cards at the time of arrest, and later analysis of historic ATM surveillance data showed that the defendant had made more than $70,000 in past attempted fraudulent EBT withdrawals from a single bank since January 2023. All three of these defendants were determined to be citizens Romania, who did not have documentation to be lawfully present in the United States. The three arrested defendants were ordered detained pending trial by the Hon. Karen Stevenson and Hon. Margo A. Rocconi. A federal grand jury returned two indictments against the three defendants for bank fraud, in violation of 18 U.S.C. § 1344; aggravated identity theft, in violation of 18 U.S.C. § 1028A; use of unauthorized access devices, in violation 18 U.S.C. § 1029(a)(2); and possession of unauthorized access devices, in violation of 18 U.S.C. § 1029(a)(3), in 23-CR-0076-FLA and 23-CR-0077-JFW.

25. In or about March 2023, federal law enforcement conducted another surveillance and arrest operation in the Los Angeles, California area. Law enforcement established surveillance around the dates when benefits had been disbursed

at select high-volume EBT fraud ATMs. Law enforcement arrested eleven suspects that conducted a high volume of unauthorized transactions and that conducted those transactions in rapid succession. At the time of their arrest, the suspects had in their possession over 400 cloned cards, $120,000 in illicitly obtained funds, and multiple skimming devices.

26. Ten out of the eleven of these defendants were determined to be citizens of Romania, who did not have documentation to be lawfully present in the United States.

C. Background of Current Operation to Combat EBT Fraud

27. The most current data provided by DSS, based in part upon reported fraud by victims, indicates that between January 2024 and January 1, 2025, more than approximately $126.8 million in cash benefits has been stolen from victim EBT cards throughout California.

28. Of the more than approximately $126.8 million in cash benefits stolen during this year time period, more than approximately $57.9 million has been stolen from victim EBT cards, in the county of Los Angeles alone. The majority of these funds were stolen through unauthorized ATM withdrawals.

29. Between on or about December 1, 2024, and on or about December 31, 2024, according to data from DSS, more than approximately $11.4 million was stolen from victim EBT cards largely through unauthorized ATM withdrawals. Of the approximately $11.4 million stolen from victim EBT cards in the month of December 2024, more than approximately $6.2 million was

stolen, mostly through unauthorized ATM withdrawals, in Los Angeles County alone.

30. Based upon my training and experience conducting access device fraud investigations, I know that suspects committing access device fraud schemes will often target particular BINs when harvesting stolen card information collected from skimming devices. Thus, suspects using skimming may target the BIN associated with DSS, in essence, targeting CalFresh and CalWORKs benefits. Moreover, based upon my training and experience, the sheer volume of unauthorized ATM withdrawals occurring during the early days of the month is further indicative that suspects participating in the fraud scheme at issue are targeting EBT cards because benefits are typically disbursed to EBT cardholders during the early days of each month.

31. Law enforcement has also reviewed ATM surveillance provided by financial institutions that administer EBT accounts that relate to the fraud scheme at issue. During the unauthorized ATM withdrawals, suspects can often be seen holding stacks of cards and conducting withdrawals in quick succession at one ATM. Based upon my training and experience, I know that suspects perpetrating access device fraud schemes will often conduct unauthorized withdrawals using cloned cards in rapid succession at ATMs.

32. Based upon the rapid succession of unauthorized ATM withdrawals being conducted, the fact that the cards being used to conduct the unauthorized cash withdrawals are nearly all

cloned EBT cards, and the fact that nearly all of the unauthorized withdrawals are happening during the early days of the month, I believe that suspects participating in the fraud scheme at issue are ostensibly targeting EBT cards.

D. CALCIU and SERBAN Committed EBT Fraud Using Unauthorized Access Devices on February 2, 2025

33. Based upon the large dollar amount being stolen from victim EBT cards, the number of victims impacted, the concentration of unauthorized ATM withdrawals occurring in particular areas, and the large number of unauthorized ATM withdrawals occurring at singular bank locations, law enforcement decided to conduct a surveillance and arrest operation in February 2025.

34. Based upon my training and experience, I know that as an anti-fraud measure, Cal DSS places an embargo on EBT accounts, such that EBT cardholders are not able to conduct cash withdrawals from their EBT cards until approximately 6:00 a.m., on the morning that their funds load (i.e., the 1st, 2nd, or 3rd of the month, depending on the account).

35. On or about February 2, 2025, beginning at approximately 6:00 a.m., law enforcement began surveillance at a U.S. Bank ATM terminal located at 11661 San Vicente Boulevard in Los Angeles, CA (the "Brentwood Square ATM"), which was identified by U.S. Bank as one of the top 30 U.S. Bank ATM locations in Los Angeles for EBT fraud. Law enforcement officers were positioned nearby such that they could see individuals walking up the ATM and conduct transactions at the

ATMs. In addition, law enforcement teams reviewed surveillance images provided by U.S. Bank of the ATM transactions from that morning.

36. Based on my review of law enforcement reports, surveillance footage, and participation during the investigation, I know that during surveillance, at approximately 6:30 a.m., law enforcement observed two individuals, (later identified as CALCIU and SERBAN) arrive in the white Volvo in front of the Brentwood Square ATM. Law enforcement observed SERBAN in the driver's seat of the white Volvo and CALCIU in the passenger's seat of the white Volvo.

37. After CALCIU exited the white Volvo and approached the Brentwood Square ATM, law enforcement observed CALCIU conduct multiple transactions which appeared to be withdrawals based upon law enforcement observing CALCIU retrieve what appeared to be currency at the conclusion of each transaction. CALCIU appeared to conduct two withdrawal transactions in rapid succession in approximately three minutes. CALCIU appeared to insert two different cards to conduct withdrawals, and put the retrieved currency and/or cards back into his pocket. Based upon my training and experience, individuals conducting legitimate transactions at ATMs typically conduct a single transaction and do not transition between multiple payment cards rapidly to conduct several transactions in a short period of time. During this time, SERBAN remained in the white Volvo.

38. While CALCIU and SERBAN were at the Brentwood Square ATM, law enforcement learned from U.S. Bank that the first

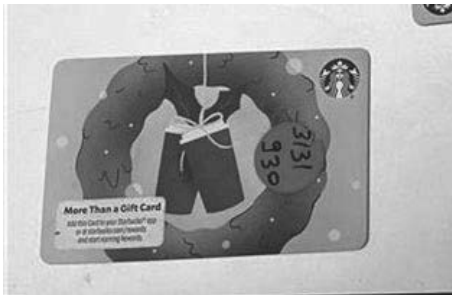
withdrawal transaction involved an EBT account belonging to a victim named M.D. Law enforcement reviewed California's Department of Motor Vehicles ("DMV") files and confirmed that the individual conducting the ATM withdrawals (CALCIU) did not appear to match the picture of M.D. in his/her DMV file. CALCIU then made an additional transaction on an EBT account belonging to an additional victim named M.S., totaling $1,300. Law enforcement similarly reviewed DMV files belonging to M.S. and confirmed that CALCIU did not match the picture of M.S.

39. Based on the date, time, ATM location, presence of multiple and successive ATM withdrawals on multiple EBT cardholder accounts during a short time period, law enforcement detained CALCIU and SERBAN in order to investigate further.

40. Based on my discussions with other law enforcement personnel, review of law enforcement reports and other evidence, and my own knowledge and participation in this investigation, I know that CALCIU and SERBAN were subsequently placed under arrest. Law enforcement searched CALCIU's and SERBAN's person.

41. CALCIU had approximately twelve access device cards in his jacket and pant pockets, ten of which were cloned to California EBT card numbers. SERBAN had approximately eight cloned EBT cards in his jacket and pant pockets. The cloned cards consisted of a variety of prepaid cards and gift cards. The cards also had stickers placed on them with, what appeared to be, based on my training and experience, card balances and victim PINs.

The following photo is an example of a seized cloned card:



42. Based on my discussions with law enforcement personnel and participation in the investigation, I know that law enforcement confirmed these were cloned EBT cards by reading the magnetic stripe and consulting with the United States Department of Agriculture Office of Inspector General to determine that the cards belonged to other real individuals, not CALCIU or SERBAN. Moreover, the cloned cards also were affixed with stickers bearing victim PIN numbers that corresponded to each cloned card and were needed in order to conduct the unauthorized ATM withdrawals.

43. Based on my review of ATM surveillance stills from U.S. Bank, I saw CALCIU perform at least two transactions involving EBT card numbers -- all of which matched EBT card numbers encoded on the cloned card seized from CALCIU incident to his arrest. These photographs clearly depicted CALCIU at the ATM conducting the unauthorized withdrawals using cloned EBT cards and directly corroborated law enforcement's surveillance observations. Two of those transactions were successful withdrawals totaling $1,300 in financial loss.

44. While CALCIU was at the ATM, SERBAN remained in the car with a large amount of cash, multiple access devices, and skimming devices. Following his arrest, law enforcement later discovered that SERBAN had cash and approximately eight access devices in his pants pocket. Law enforcement later searched the white Volvo and learned that SERBAN, while serving as the driver of the white Volvo, was also in possession of cash and approximately sixty-one additional access devices in the white Volvo.

45. During processing, when asked to identify himself, CALCIU provided the name "Ionut" and produced a Washington driver's license bearing the name "Ionut CALCIU" and birth date of "June 18, 1993." Law enforcement queried CALCIU in U.S. Immigration and Customs Enforcement ("ICE") databases and learned that CALCIU had no lawful status in the United States. Based on my review of law enforcement database records, I learned that CALCIU had a criminal history dating back to 2022 in the United States. CALCIU's criminal history in the United States included misdemeanor charges for theft/petty theft merchandise, manufacturing false identification documents, conspiracy to commit a crime, possession of burglary tools, destroying/concealing evidence and multiple felony charges for identity theft, possession of identification of 10+ persons with intent to defraud, counterfeiting credit cards, and grand theft.

46. During processing, when asked to identify himself, SERBAN provided the name "Florian SERBAN." SERBAN produced a California State driver's license and an Employment

Authorization card, both bearing the name "Florian SERBAN" and birth date of "September 10, 1973." Law enforcement queried SERBAN in ICE databases and learned that SERBAN had an approved Employment Authorization (I-756) with the approval date of December 12, 2024. SERBAN stated he had an asylum application pending, which was verified by ICE. Based on my review of law enforcement database records, I learned that SERBAN had a criminal history dating back to 1994 in Europe, 2006 in Romania, and 2024 in the United States. SERBAN's criminal history in Europe included multiple charges for use of false documents. Specifically, SERBAN's criminal history in Romania included possession of high-risk drugs, illegal operations with devices or software, creation of an organized crime group, murder, and aggravated murder. SERBAN's criminal history in the United States include charges of unauthorized use of another person's personal identifying information and unlawful factoring of a credit card transaction.

47. Based on my training and experience, I know that criminals conducting access device fraud schemes will often conceal their true identities by obtaining fictitious IDs to enter the country illegally while evading law enforcement.

48. SUBJECT DEVICE 1 was retrieved from CALCIU's pockets, and SUBJECT DEVICE 2 was retrieved from SERBAN's pockets prior to arrest. The SUBJECT DEVICES are currently in the custody of USSS in Los Angeles pending issuance of a search warrant.

49. After being advised of their Miranda rights, which were printed in Romanian, CALCIU and SERBAN chose not to speak

with law enforcement. Law enforcement ceased any questioning of CALCIU and SERBAN after both indicated they would like to speak with a lawyer.

V. TRAINING AND EXPERIENCE REGARDING IDENTITY THEFT CRIMES

50. Based on my training and experience and information obtained from other law enforcement officers who investigate identity theft, I know the following:

a. It is common practice for individuals involved in identity theft, bank fraud, and access device fraud crimes to possess and use multiple digital devices at once. Such digital devices are often used to facilitate, conduct, and track fraudulent transactions and identity theft. Suspects often use digital devices to perpetrate their crimes due to the relative anonymity gained by conducting financial transactions electronically or over the internet. They often employ digital devices for the purposes, among others, of: (1) applying online for fraudulent credit cards; (2) obtaining or storing personal identification information for the purpose of establishing or modifying fraudulent bank accounts and/or credit card accounts; (3) using fraudulently obtained bank accounts and/or credit card accounts to make purchases, sometimes of further personal information; (4) keeping records of their crimes; (5) researching personal information, such as social security numbers and dates of birth, for potential identity theft victims; and (6) verifying the status of stolen access devices.

b. Oftentimes identity thieves take pictures of items reflecting their stolen identities, including items

retrieved from stolen mail or mail matter, with their cellphones.

c. It is also common for identity thieves to keep "profiles" of victims on digital devices. Such "profiles" contain the personal identifying information of victims, such as names, Social Security numbers, dates of birth, driver's license or state identification numbers, alien registration numbers, passport numbers, and employer or taxpayer identification numbers. Identity thieves often keep such information in their cars, storage units, and in their digital devices.

d. It is common for identity thieves, and individuals engaged in bank fraud, access device fraud, and identification document fraud to use equipment and software to print credit and identification cards, to create magnetic strips for credit cards, to use embossing machines to create credit cards, to use laser printers to create checks, and to use magnetic card readers to read and re-encode credit cards. These types of devices are routinely kept where the person will have easy access to such devices, such as on their person or in their cars or homes or storage units. Software relevant to such schemes can also often be found on digital devices, such as computers.

e. Based on my training and experience, I know that individuals who participate in identity theft, bank fraud, and access device fraud schemes often have co-conspirators, and often maintain telephone numbers, email addresses, and other contact information and communications involving their co-

conspirators in order to conduct their business. Oftentimes, they do so on their digital devices. Suspects often use their digital devices to communicate with co-conspirators by phone, text, email, and social media, including sending photos. Suspects may also have paper copies of such records, which they may keep on their person or in their cars, homes, or storage units.

f. Individuals engaged in mail and identity theft often use multiple digital devices, which they may keep on their person or in their cars.

VI. TRAINING AND EXPERIENCE ON DIGITAL DEVICES[1]

51. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur

[1] As used herein, the term "digital device" includes the SUBJECT DEVICES as well as any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as paging devices, mobile telephones, and smart phones; digital cameras; gaming consoles; peripheral input/output devices, such as keyboards, printers, scanners, monitors, and drives; related communications devices, such as modems, routers, cables, and connections; storage media; and security devices.

after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain

"booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

52. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

53. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

VII. CONCLUSION

54. For all of the reasons described above, there is probable cause to believe that CALCIU and SERBAN have committed a violation of 18 U.S.C. § 1029(a)(2) (use of unauthorized access devices). There is also probable cause that the items to be seized described in Attachment B will be found in a search of the SUBJECT DEVICES as described in Attachment A.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 3 day of February, 2025.

HONORABLE MARGO A. ROCCONI
UNITED STATES MAGISTRATE JUDGE